UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,960	11/06/2000	Scott A. Cluff	MICE-0091-US(00.00902)	8488

7590 12/23/2004

Dan C Hu
Trop Pruner & Hu PC
8554 Katy Freeway
Suite 100
Houston, TX 77024

EXAMINER	
CHU, GABRIEL L	

ART UNIT	PAPER NUMBER
2114	

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/706,960	CLUFF ET AL.	
	Examiner	Art Unit	
	Gabriel L. Chu	2114	

-- The MAILING DATE of this communication appears on the cover sh et with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18-20,24-26 and 28-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 18-20 24-26 28-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

STATUS OF CLAIMS

1. Claims 1, 2, 4-7, 9-11, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 5627964 to Reynolds et al.

2. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over over US 5713024 to Halladay in further view of US 5627964 to Reynolds et al. as applied to claim 1 above, in further view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens.

3. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 5627964 to Reynolds as applied to claim 1 above, and further in view of US 6381694 to Yen.

4. Claims 12-16 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens.

5. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens as applied to claim 12 above, and further in view of US 4972316 to Dixon et al.

6. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens as applied to claim 12 above, and further in view of US 5627964 to Reynolds et al.

7. Claims 28 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 4972316 to Dixon et al. and US 5627964 to Reynolds et al.

8. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 4972316 to Dixon et al. and "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens.

9. Claims 17, 21-23, and 27 are cancelled.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1, 2, 4-7, 9-11, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 5627964 to Reynolds et al. Referring to claim 1, Halladay discloses an interface to a network (Figure 1, elements 2, 5, 6, 16, and the communication path between 16 and 20.); a first operational element to perform one or more tasks in the system (From the abstract, "This apparatus automatically formats the computer system memory in response to a failure thereof and automatically restores the operating system, all application programs and every data file that is selected by the user to be monitored and preserved by this apparatus."); and a backup device to enable access of the network through the interface in response to failure of the first operational element (From line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media

21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer system 1 or a data communication port 6. The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3."). Although Halladay do not specifically disclose a storage element containing a flag to indicate if a fault has occurred with the first operational element, using a flag that indicates a fault so as to initiate a recovery program is well known in the art. An example of this is shown by Reynolds et al., from line 20 of column 6, "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output components are a subset of core components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." A person of ordinary skill in the art at the time of the invention would have been motivated to indicate a failure to initiate recovery because, from line 29 of column 6, "indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode".

12. Referring to claim 2, Halladay discloses the first operational element comprises a disk drive (From line 59 of column 4, "In a personal computer, this backup is a dump of the contents of the hard drive.").

13. Referring to claim 4, Halladay discloses the backup routine comprises a browser (From line 3 of column 5, "The user accesses the cold boot data backup system 10 via the standard application program activation process native to computer system 1. The cold boot data backup system 10, when activated, presents the user with the display illustrated in FIG. 2. The configuration selection activates the capability for the user to define the mode of data backup and to identify the elements that are to be protected. This process is similar to existing data backup systems and is not described in great detail herein in the interest of brevity and clarity of description.").

14. Referring to claim 5, Halladay discloses the first operational element comprises a first disk drive, and wherein the backup storage element comprises a second disk drive separate from the first disk drive (From line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media 21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer system 1 or a data communication port 6. The backup device 20 can be collocated with computer system

1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3.").

15. Referring to claim 6, Halladay discloses the second disk drive has a smaller storage capacity than the first disk drive (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored.").

16. Referring to claim 7, Halladay discloses the backup storage element comprises non-volatile memory (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored.").

17. Referring to claim 9, Halladay discloses the backup device comprises a removable disk drive (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored.").

18. Referring to claim 10, Halladay discloses the backup device to retrieve user data and software over the network to recover the system (From line 45 of column 8, "The

cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read." Further, from line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media 21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer system 1 or a data communication port 6. The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3." Further, from line 67 of column 7,

"The cold boot apparatus 10 populates the cold boot floppy disk with the required programs and data to execute the hard drive restore process.").

19. Referring to claim 11, Halladay discloses the first operational element comprises a storage element, the backup device to retrieve an image of the storage element to recover the storage element to its operational state (From line 55 of column 4, "A primary function of the cold boot data backup system 10 is to backup data files that are created and modified by the user on to a backup media 21 for safekeeping. To accomplish this goal, it is expected that a user first backs up the entirety of the data stored in the memory of computer system 1. In a personal computer, this backup is a dump of the contents of the hard drive." Further, from line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base.").

20. Referring to claim 30, Halladay in view of Reynolds et al. discloses a BIOS routine to detect a state of the flag, the BIOS routine to access the backup device in response to detecting that the flag indicates the fault (From line 20 of column 6 of Reynolds et al., "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output components are a subset of core components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." Further, from line 42 of column 6 of Reynolds et al., "If either the flag is set (Step AC) or a command to load the fail-safe mode was received (Step AD), the flag is cleared (Step AE), and minimal drivers 203 and required drivers 204 are loaded along with any of the core components 201 not already loaded as basic input-output components (Step AF). Thereafter, applications programs can be executed with the limited functionality provided by the minimal and required drivers (Step AG)." Further, from line 45 of column 8 of Halladay, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at

step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21.").

21. Referring to claim 31, Halladay discloses the software comprises operating system software (Figure 1, element 19.).

22. Referring to claim 32, Halladay in view of Reynolds et al. discloses the backup device is adapted to retrieve an image containing user data and operating system software over the network in response to the flag (From line 20 of column 6 of Reynolds et al., "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output components are a subset of core components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." Further, from line 42 of column 6 of Reynolds et al., "If either the flag is set (Step AC) or a command to load the fail-safe mode was received (Step AD), the flag is cleared (Step AE), and minimal drivers 203 and required drivers 204 are loaded along with any of the core components 201 not already loaded as basic input-output components (Step AF). Thereafter, applications programs can be executed with the limited functionality provided by the minimal and required drivers (Step AG)." Further, from line 45 of column 8 of Halladay, "The cold boot application program at step 86 next

initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21.").

23. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over over US 5713024 to Halladay in further view of US 5627964 to Reynolds et al. as applied to claim 1 above, in further view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens. Referring to claim 3, Halladay discloses the backup device comprises a backup storage element containing a backup routine adapted to perform communications through the interface to the network (From line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media 21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer system 1 or a data communication port 6. The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3."). Although Halladay in view of Reynolds et al. does not specifically disclose the interface comprises a network stack having an IP layer, using IP in networking is extremely well known in the art. An

example of this is shown by Stevens, from page 1, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe." A person of ordinary skill in the art at the time of the invention would have been motivated to use IP because from page 1 of Stevens, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe."

24. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 5627964 to Reynolds as applied to claim 1 above, and further in view of US 6381694 to Yen. Referring to claim 8, although Halladay in view of Reynolds et al. do not specifically disclose the first operational element comprises a disk drive having plural partitions, and wherein the backup device comprises one of the partitions, using a partition for recovery is known in the art. An example of this is shown by Yen, from line 66 of column 1, "In accordance with the present invention, the foregoing objective is achieved by means of a user-hidden secondary volume or partition in the computer permanent storage mechanism, e.g., hard disk. If an error is detected which would normally result in an operational failure, the computer branches to recovery software stored in the secondary volume. For

example, in the case of startup errors, the recovery software can include an alternate startup application which enables the computer to be booted. In one embodiment, the startup application installs a minimal operating system on the primary volume and then restarts the computer. Due to the presence of the minimal operating system installed in the primary volume, the computer is able to start. As a result, the user is not left with a non-functioning computer." A person of ordinary skill in the art at the time of the invention would have been motivated to have a second partition for recovery because, from line 17 of column 4, "The recovery software is located in a separate area of permanent storage, rather than the main area, to ensure its reliability."

25. Claims 12-16 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens. Claims 12-16 and 18-20 are rejected under 35 U.S.C. 102(b) as being anticipated by US 5713024 to Halladay. Referring to claim 12, Halladay discloses detecting if an operating portion of the system has experienced a fault (From line 57 of column 1, "If a failure occurs, the cold boot data backup system performs the data file location, retrieval and restore operations, independent of the user."); accessing a backup device to enable communication over a network (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at

step 86B to read the directory information from this backup media 21." Further, from line 41 of column 3, "The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3."); retrieving data over the network, the data comprising an image containing user data and an operating system (From line 53 of column 8, "The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above."); and recovering the system using the image (From line 57 of column 8, "The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read."). Although Halladay does not specifically disclose the network for communication and retrieving uses a network stack including an Internet Protocol (IP) layer, using IP in networking is extremely well known in the art. An example of this is shown by Stevens, from page 1, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe." A person of ordinary skill in the art at the time of the invention would have been motivated to use IP because from page 1 of Stevens,

"The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe."

26. Referring to claim 13, Halladay discloses loading a backup software routine from the backup device (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored.").

Referring to claim 14, Halladay in view of Stevens discloses the backup software routine comprises a browser, the method further comprising executing the browser to access the network through the network stack including the IP layer to retrieve the data (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and

incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read.").

Referring to claim 15, Halladay discloses executing the backup software routine to access the network (From line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media 21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer system 1 or a data communication port 6. The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3.").

Referring to claim 16, Halladay discloses retrieving the data comprises retrieving the data from a backup storage system couple to the network (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from

this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read.").

Referring to claim 18, Halladay discloses booting from a backup storage device instead of the main storage device if the system has experienced a fault (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored."); using the backup storage device to enable communications over a network to retrieve an image to recover the system, wherein the image comprises user data and an operating system (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for

full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read." Further, from line 41 of column 3, "The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3."). Although Halladay does not specifically disclose the network uses a network stack including an Internet Protocol (IP) layer, using IP in networking is extremely well known in the art. An example of this is shown by Stevens, from page 1, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe." A person of ordinary skill in the art at the time of the invention would have been motivated to use IP because from page 1 of Stevens, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe."

Referring to claim 19, Halladay in view of Stevens discloses loading a routine from the backup storage device to enable the network communication through the network stack including the IP layer (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read." Further, from line 32 of column 3, "The cold boot data backup apparatus 10 is installed on computer system 1 and serves to store selected data files on a backup media 21 that is located in backup drive 20. The backup media 21 is a rewriteable media, and can be mountable magnetic tape, fixed disk drive media, mountable disk drive media, disk drive array, or any other rewriteable media. The backup drive 20 is typically a separate device that is connected to computer system 1 via an interface, such as the parallel port 5 of the computer

system 1 or a data communication port 6. The backup device 20 can be collocated with computer system 1 or can be located remote from computer system 1 and connected thereto via a data communication link 7 or network 3." Further, from line 67 of column 7, "The cold boot apparatus 10 populates the cold boot floppy disk with the required programs and data to execute the hard drive restore process.").

Referring to claim 20, Halladay discloses loading the routine comprises loading a browser (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read.").

27. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W.

Richard Stevens as applied to claim 12 above, and further in view of US 4972316 to Dixon et al. Referring to claim 24, Halladay discloses in response to the fault, formatting a storage device and subsequently storing image data in the storage device (From line 22 of column 8, 'The cold boot process is typically initiated by the user in response to the failure of the hard drive, which has caused the loss of all the data and application programs that were stored thereon. The user initiates the cold boot process, which is illustrated in flow diagram form in FIG. 8, by loading the cold boot floppy disk into the floppy drive of the computer system at step 81. At step 82, the user boots the computer system 1, which searches the hard drive and the cold boot floppy disk for the proper startup program. The computer system 1 identifies the floppy disk as a bootable disk and reads the cold boot disk to locate the auto.sub.-- exec.bat file written thereon. The computer system 1, at step 83, reads the auto.sub.-- exec.bat file from the cold boot floppy disk, which auto.sub.-- exec.bat file directs the computer system 1 to the cold boot application program that is written on the cold boot floppy disk. At step 84, the computer system 1 executes the cold boot application program, which instructs the computer system 1 to run the disk format operation, which is also stored on the cold boot floppy disk, on the newly installed hard drive. At step 85, the computer system 1 reads the disk format program from the cold boot floppy disk and initiates a hard drive format process which formats the hard drive in well-known fashion and restores the hard drive parameters, establishing partitions, etc. The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive

immediately prior to the hard drive failure."). Although Halladay does not specifically disclose this formatting comprises scanning a storage device to determine portions of the storage device that are defective; and storing the image in portions of the storage device other than the portions that are defective, mapping out defective portions of a disk during formatting is well known in the art. An example of this is shown by Dixon et al., from line 50 of column 1, "One problem that is known in the art, arises because of the fact that defects exist in the disk storage media. Thus, sectors containing such defects are considered bad and cannot be used. Such bad sectors are normally identified by formatting and later uses thereof avoided by simply skipping a bad sector." A person of ordinary skill in the art at the time of the invention would have been motivated to map out a bad sector because, from line 52 of column 1 of Dixon et al. "sectors containing such defects are considered bad and cannot be used".

28. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens as applied to claim 12 above, and further in view of US 5627964 to Reynolds et al. Referring to claim 25, although Halladay does not specifically disclose setting a flag in response to detecting the operating portion of the system has experienced a fault; and a BIOS routine to detect whether the flag has been set, using a BIOS to detect a flag that indicates failure is well known in the art. An example of this is shown by Reynolds et al., from line 20 of column 6, "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output

components are a subset of core components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." A person of ordinary skill in the art at the time of the invention would have been motivated to indicate a failure to initiate recovery because, from line 29 of column 6, "indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode".

Referring to 26, Halladay in view of Reynolds et al. discloses the BIOS routine to access the backup device to load a routine for communicating over the network in response to detecting that the flag has been set (From line 42 of column 6, "If either the flag is set (Step AC) or a command to load the fail-safe mode was received (Step AD), the flag is cleared (Step AE), and minimal drivers 203 and required drivers 204 are loaded along with any of the core components 201 not already loaded as basic input-output components (Step AF). Thereafter, applications programs can be executed with the limited functionality provided by the minimal and required drivers (Step AG)." Further, from line 45 of column 8 of Halladay, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at

step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21.").

29. Claims 28 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 4972316 to Dixon et al. and US 5627964 to Reynolds et al. Referring to claim 27, Halladay discloses a system to detect if an operating portion of the system has experienced a fault (From line 57 of column 1, "If a failure occurs, the cold boot data backup system performs the data file location, retrieval and restore operations, independent of the user."); access a backup device to enable communication over a network (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21."); retrieve data to recover the sytem over the network, the data comprising an image containing user data and operating system software (From line 53 of column 8, "The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above."); and recovering the system using the image (From line 57 of column 8, "The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process

of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read."). Halladay further discloses in response to the fault, formatting a storage device and subsequently storing image data in the storage device (From line 22 of column 8, 'The cold boot process is typically initiated by the user in response to the failure of the hard drive, which has caused the loss of all the data and application programs that were stored thereon. The user initiates the cold boot process, which is illustrated in flow diagram form in FIG. 8, by loading the cold boot floppy disk into the floppy drive of the computer system at step 81. At step 82, the user boots the computer system 1, which searches the hard drive and the cold boot floppy disk for the proper startup program. The computer system 1 identifies the floppy disk as a bootable disk and reads the cold boot disk to locate the auto.sub.-- exec.bat file written thereon. The computer system 1, at step 83, reads the auto.sub.-- exec.bat file from the cold boot floppy disk, which auto.sub.-- exec.bat file directs the computer system 1 to the cold boot application program that is written on the cold boot floppy disk. At step 84, the computer system 1 executes the cold boot application program, which instructs the computer system 1 to run the disk format operation, which is also stored on the cold boot floppy disk, on the newly installed hard drive. At step 85, the computer system 1 reads the disk format program from the cold boot floppy disk and initiates a hard drive format process which formats the hard drive in well-known fashion and restores the hard drive parameters, establishing partitions, etc. The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with

all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure.").

Although Halladay does not specifically disclose this formatting comprises scanning a storage device to determine portions of the storage device that are defective; and storing the image in portions of the storage device other than the portions that are defective, mapping out defective portions of a disk during formatting is well known in the art. An example of this is shown by Dixon et al., from line 50 of column 1, "One problem that is known in the art, arises because of the fact that defects exist in the disk storage media. Thus, sectors containing such defects are considered bad and cannot be used. Such bad sectors are normally identified by formatting and later uses thereof avoided by simply skipping a bad sector." A person of ordinary skill in the art at the time of the invention would have been motivated to map out a bad sector because, from line 52 of column 1 of Dixon et al. "sectors containing such defects are considered bad and cannot be used".

Although Hallday in view of Dixon et al. do not specifically disclose a system to set a flag in response to the fault; load a BIOS routine to detect whether the flag is set; and cause the BIOS routine to load a second routine in response to detecting the flag is set, using a BIOS to detect a flag that indicates failure, and do something in response, is well known in the art. An example of this is shown by Reynolds et al., from line 20 of column 6, "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output components are a subset of core

components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." Further, from line 42 of column 6, "If either the flag is set (Step AC) or a command to load the fail-safe mode was received (Step AD), the flag is cleared (Step AE), and minimal drivers 203 and required drivers 204 are loaded along with any of the core components 201 not already loaded as basic input-output components (Step AF). Thereafter, applications programs can be executed with the limited functionality provided by the minimal and required drivers (Step AG)." Further, from line 45 of column 8 of Halladay, "The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21."A person of ordinary skill in the art at the time of the invention would have been motivated to indicate a failure to initiate recovery because, from line 29 of column 6, "indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode".

30. Referring to claim 33, Halladay in view of Dixon et al. discloses storing the retrieved data comprises storing the retrieved image containing user data and operating system software in the portions of the storage device other than the portions that are identified to be defective by the scan (From line 50 of column 1 of Dixon et al., "One problem that is known in the art, arises because of the fact that defects exist in the disk storage media. Thus, sectors containing such defects are considered bad and cannot be used. Such bad sectors are normally identified by formatting and later uses thereof avoided by simply skipping a bad sector.").

31. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 5713024 to Halladay in view of US 4972316 to Dixon et al. and "Introduction" from TCP/IP Illustrated, Volume 1 by W. Richard Stevens. Referring to claim 29, Halladay discloses a main storage device (From line 59 of column 4, "In a personal computer, this backup is a dump of the contents of the hard drive."); a backup storage device, a first routine executable to boot from the backup storage device in case of a system fault (From line 57 of column 7, "The cold boot apparatus 10 typically consists of an application program resident on computer system 1, which is used as described herein to create a cold boot floppy disk which is used to cold boot the computer system I in the event the memory of computer system 1 false and must be completely restored."), the backup storage device enabling access over a network to retrieve data from a network to recover the system, wherein the retrieved data comprises an image containing user data and operating system software (From line 45 of column 8, "The cold boot application program at step 86 next initiates the hard drive restore process which

populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure. The cold boot program instructs the user at step 86A to load the first backup media 21 into the backup drive 20 and proceeds at step 86B to read the directory information from this backup media 21. The backup media 21 is searched for full and incremental backup sessions, each of which are identified via system IDs in the ID history that was written by the cold boot apparatus 10 on the cold boot floppy disk as noted above. The data that is retrieved from the backup media 21 regarding the full and incremental backup sessions are used by the cold boot program at step 86C to create a temporary data base. The backup media read process of steps 86A and 86B are repeated for each backup media that has been created for the computer system 1 until at step 86C it is determined that the last backup media 21 has been read.").Halladay further discloses in response to the fault, a second routine to format a storage device and subsequently store image data in the storage device (From line 22 of column 8, 'The cold boot process is typically initiated by the user in response to the failure of the hard drive, which has caused the loss of all the data and application programs that were stored thereon. The user initiates the cold boot process, which is illustrated in flow diagram form in FIG. 8, by loading the cold boot floppy disk into the floppy drive of the computer system at step 81. At step 82, the user boots the computer system 1, which searches the hard drive and the cold boot floppy disk for the proper startup program. The computer system 1 identifies the floppy disk as a bootable disk and reads the cold boot disk to locate the auto.sub.-- exec.bat file written thereon. The computer system 1, at

step 83, reads the auto.sub.-- exec.bat file from the cold boot floppy disk, which auto.sub.-- exec.bat file directs the computer system 1 to the cold boot application program that is written on the cold boot floppy disk. At step 84, the computer system 1 executes the cold boot application program, which instructs the computer system 1 to run the disk format operation, which is also stored on the cold boot floppy disk, on the newly installed hard drive. At step 85, the computer system 1 reads the disk format program from the cold boot floppy disk and initiates a hard drive format process which formats the hard drive in well-known fashion and restores the hard drive parameters, establishing partitions, etc. The cold boot application program at step 86 next initiates the hard drive restore process which populates the hard drive with all the application programs and application data to recreate the state of the hard drive immediately prior to the hard drive failure.").

Although Halladay does not specifically disclose this formatting comprises scanning a storage device to determine portions of the storage device that are defective; and storing the image in portions of the storage device other than the portions that are defective, mapping out defective portions of a disk during formatting is well known in the art. An example of this is shown by Dixon et al., from line 50 of column 1, "One problem that is known in the art, arises because of the fact that defects exist in the disk storage media. Thus, sectors containing such defects are considered bad and cannot be used. Such bad sectors are normally identified by formatting and later uses thereof avoided by simply skipping a bad sector." A person of ordinary skill in the art at the time of the invention would have been motivated to map out a bad sector because,

from line 52 of column 1 of Dixon et al. "sectors containing such defects are considered bad and cannot be used".

Although Halladay in view of Dixon et al. does not specifically disclose the network comprises a network stack having an IP layer, using IP in networking is extremely well known in the art. An example of this is shown by Stevens, from page 1, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe." A person of ordinary skill in the art at the time of the invention would have been motivated to use IP because from page 1 of Stevens, "The TCP/IP protocol suite allows computers of all sizes, from many different computer vendors, running totally different operating systems, to communicate with each other.... It forms the basis for what is called the worldwide Internet, or the Internet, a wide area network (WAN) of more than one million computers that literally spans the globe."

Response to Arguments

32. Applicant's arguments filed 5 October 2004 have been fully considered but they are not persuasive. Regarding Applicant's argument (page 8) that in Halladay, figure 1 depicts a backup drive 20 connected to a port of the computer 1, Halladay also both shows in illustration and in the written detailed embodiments that backup drive 20 may be accessed across a network (see above rejections).

33. Regarding Applicant's argument (page 8) that Halladay in view of Reynolds et al. does not disclose a flag to indicate fault and a backup device to access the network in response to the flag indicating fault, as in the rejection above, using a flag that indicates a fault so as to initiate a recovery program is well known in the art. An example of this is shown by Reynolds et al., from line 20 of column 6, "First, the computer system 101 is started up (Step AA). Next, basic input-output components of the operating system are loaded (Step AB), for example, into portions of memory 107. The basic input-output components are a subset of core components 201 sufficient to enable processor 105 to check the special flag (in Step AC, below). They can include, for example, components to access storage mechanism 108. Next, processor 105 determines whether a special flag is set (Step AC). This flag indicates whether fail-safe mode is to be established in response to a previous failure of an attempt to establish normal mode. The flag can be stored, for example, using storage mechanism 108." Applicant appears to be arguing against bodily incorporation.

The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Using a Boolean indication means to indicate a failure/fault that needs to be responded to by some means is extremely and notoriously well known in the art.

Examiner has provided one such example, which may or may not be bodily incorporated, to show this concept to Applicant. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

34. Regarding Applicant's argument (page 9) that Halladay specifically teaches the use of a floppy disk wherein loading itself acts for starting the restoring process, see paragraph 33 regarding bodily incorporation and piecemeal analysis.

35. Regarding Applicant's argument (page 10) that Reynolds et al. is not concerned with restoring data from a backup device, again, the Reynolds et al. is merely provided to show the concept of using a flag to indicate fault and initiate fault recovery, a very well known concept, taken in combination with the teachings of Halladay.

Conclusion

36. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gabriel L. Chu whose telephone number is (571) 272-3656. The examiner can normally be reached on weekdays between 8:30 AM and 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel, Jr. can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

gc

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100